Western Technical College

10150119 Network Security 2

Course Outcome Summary

Course Information

Description	Provides hands-on training and exposure to information security management techniques and information assurance tools. Students will complete lab and project-based activities enabling them to defend systems, networks, and applications against practical and viable computing threats. Students will also learn countermeasures for defending the network infrastructure through real-life situational training exercises. Topics include intrusion detection and prevention systems (IDS/IPS), firewalls, log collection, e-Discovery/forensics, incident response, anomaly detection, content filtering, system hardening, malware analysis, and encryption.
Career Cluster	Information Technology
Instructional Level	Associate Degree Courses
Total Credits	3
Total Hours	90

Textbooks

No textbook required.

Program Outcomes

1. Implement computer networks.
2. Implement client systems.
3. Implement server operating systems.
4. Implement network security components.
5. Develop technical documentation.
6. Troubleshoot network systems.

Course Competencies

1. Install an eventlog monitoring/management solution

Assessment Strategies

1.1. Project evaluation

Criteria

You will know you are successful when:

1.1. you deploy a directory server and configure a functional account audit solution.
1.2. you demonstrate competent use of the of the EventLog and identification of EventID types.
1.3. you develop an effective SQL query and TPL report to detect account anomalies

Learning Objectives

1.a. Employ domain policy to audit and record logon failures.
1.b. Develop SQL queries to retrieve security event ID

2. Install an IIS W3C log monitoring and management solution.

Assessment Strategies

2.1. Project Evaluation

Criteria

You will know you are successful when:

2.1. you configure a functional IIS webserver
2.2. you configure W3C logging parameters
2.3. you implement a vulnerability scan against your IIS webserver
2.4. you develop a script to detect anomalies generated by the vulnerability scan

Learning Objectives

2.a. Employ W3C logging
2.b. Develop a script to detect anomalies in the log file.

3. Utilize digital forensic utilities and perform eDiscovery

Assessment Strategies

3.1. Project Evaluation

Criteria

You will know you are successful when:

3.1. you successfully capture a forensic image
3.2. you mount the captured image and perform an analysis
3.3. you successfully detect criminal activity in the mounted image

Learning Objectives

3.a. Perform forensic image capture.
3.b. Implement captured image parse.
3.c. Perform file carving and extract relevant data.

4. Design and implement an incident response kit (IRK).

Criteria

You will know you are successful when:

4.1. you research and acquire the baseline tools for a response kit
4.2. you create a script to automate incident response tool execution and outfile storage
4.3. you design and implement a report to efficiently analyze the data captured by the incident response tools

Learning Objectives

4.a. Identify utilities approved by the industry for litigation use
4.b. Assemble utilities required for incident capture and reporting
4.c. Implement a scripted solution that executes from a write block USB device

5. Install a hardware firewall.

Criteria

You will know you are successful when:

5.1. you have installed the firewall OS on the provided 1U server
5.2. you have performed an initial configuration to allow users to access the internet
5.3. you have successfully configured failover to a secondary internet service provider

Learning Objectives

5.a. Install a functional firewall OS to a 1U server
5.b. Administer the system to allow user access to the internet
5.c. Employ fail-over configuration to a secondary service provider

6. Employ an enterprise monitoring utility.

Criteria

You will know you are successful when

6.1. you research, install and configure a monitoring solution for your chosen platform.
6.2. you boot from the live MEDIA and configure the monitoring solution for key internet services.
6.3. you are accurately notified when a service is stopped or suspended.

Learning Objectives

6.a. Create a baseline to determine normal network activity
6.b. Set up up trigger events to monitor baseline services
6.c. Test the triggers to verify notification of service failure